UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/750,511	12/27/2000	Balas Natarajan Kausik	028410-0002 DIV	6911

20350 7590 04/06/2004

TOWNSEND AND TOWNSEND AND CREW, LLP
TWO EMBARCADERO CENTER
EIGHTH FLOOR
SAN FRANCISCO, CA 94111-3834

EXAMINER	
SEAL, JAMES	
ART UNIT	**PAPER NUMBER**
2135	

DATE MAILED: 04/06/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/750,511	KAUSIK, BALAS NATARAJAN	
	Examiner	Art Unit	
	James Seal	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 December 2000*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *98* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *98* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This Action is in response to applicant's correspondence of 27 December 2000.

2. IDS was considered by the examiner and a signed copy is returned with this action.

3. Amendament to specification have been entered.

4. Claims 1-97 have been cancelled.

5. Claim 98 has been added.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claim 98 is rejected under 35 U.S.C. 103(a) as being unpatentable over Ganesan US 5535276, and further in view of Johnson et. al. US 5815573 and Matyas et. al. US 5142578 A.

8. As per claim 98, the limitation of dividing an exponent d of the private key of a public key cryptosystem into two portions is taught by Ganesan in "Communications using Split Private Key Asymmetric Cryptography" (see Column 2, lines 62-64). Ganesan is silent on the limitation that the key should be divided into a most significant portion and a least significant portion.

9. Johnson teaches breaking a key (a number) into two or more portions which are related to the bit size, for the purpose of allowing law enforcement agencies in countries

in which strong encryption (say 56 bit DES) is forbidden but 40 bit encryption (weak) DES is permit. This is done by splitting the key and giving a portion related to the size of the key to the law enforcement agency and another portion related to the size of the key is kept by the user (see Column 6, lines 61-67and Column 7, lines 1-7, Figure 1). As the number of bits is chosen to break into portions is chosen from left to right (or right to left, little or big Endian systems) the portions are selected according to most and least significance (Column 7, lines 4-7). One of ordinary skill in the art at the time the invention was made would have been motivated to use the teachings of Johnson in combination with those of Genesan because manipulations of bits by a computer and in particular selecting a least significant portion or a most significant portion is only a material of position in the register.

10. The limitation of storing in a secure database is taught by Ganesan (Column 14, lines 33-34), but Genesan and Johnson are silent on how the database is secured.

11. Matyas discloses the use of Secure key management employment key encrypt key (KEK) storage as the preferred way for secure key storage (Column 2, line 66-68 and Column 3, lines 1-18). One of ordinary skill in the art at the time the invention was made would have been motivated to combine the teaching of Genesan/Johnson with those Matyas in particular key storage has the following two problems: keys are short data strings and keys must be entered and extracted quiet frequently. By encrypting individual keys rather than the entire data, one conserves resources when a key must be entered or extracted. Further Matytas further discloses concatenating the key with identification material (a control vector). One of ordinary skill in the art at the time the

invention was made would have been motivated to further combine the teachings of concatenating the encrypted key with identification material such as a password or PIN or in the form of identification material that only the user would have that is the other half of the key. Claim 98 is rejected.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to James Seal whose telephone number is 703 308 4562. The examiner can normally be reached on M-F, 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 703 305 4393. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

James Seal
AU 2135
2 April 2004